

**STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

We download so much of our daily lives into our mobile devices. Those devices are in our palms, pockets, and purses—they're with us always. They provide us with connections a million times more powerful than what was available on Apollo 11. It's pretty incredible. It also makes them a terrific target for fraud.

One of the most dangerous scams is called SIM swapping fraud. SIM cards are small plastic chips, about the size of a dime, that are inserted into a mobile phone to identify and authenticate the subscriber.

SIM cards are increasingly at the center of scams involving our mobile devices. Here's how it works: A fraudster calls up your wireless provider and convinces the customer service representative that they are you and need your phone number switched to a new SIM card that they control. These cybercrooks do not need your phone to do this, they simply need to convince your carrier to make a change to your account. Once they do, they can use your phone number to divert your incoming messages and easily complete the kind of two-factor authentication checks that financial institutions and social media companies use. They also can be used to take over your e-mail and drain your bank accounts.

By all accounts, including a big, recent Princeton University study, this type of fraud is growing. At the Federal Communications Commission, we've seen complaints from consumers who have suffered significant distress, inconvenience, and financial harm because of SIM swapping. To make matters worse, recent carrier data breaches that have made headlines may have exposed the very kind of customer information that could make it easier to pull off these kinds of attacks.

As Senator Ron Wyden has said, "Consumers are at the mercy of wireless carriers when it comes to being protected against SIM swaps." He's right. But we have tools at this agency we can use so consumers are better protected, and their devices are more secure. In fact, we have rules on the books designed to prevent your carrier from sharing personal and private information. These rules govern how carriers are supposed to protect what is known in the law as customer proprietary network information, or CPNI. But these rules need an update to address new types of fraud like SIM swapping.

That's what we start here today. We propose to update our CPNI and related local number portability rules to require carriers to securely authenticate a customer before transferring a phone number to a new device or carrier, and we seek comment on the best way to do that. We also propose that carriers immediately notify customers whenever a SIM change or port request has been made. These proposals will help protect consumers from both SIM swaps and a related kind of fraud known as "port-out fraud," where fraudsters pose as their victims and then arrange to transfer their victim's phone number to a new account that they control.

It's important we do this now. The Princeton University study I mentioned found that four out of five SIM swap attempts in the United States are successful. We can help fix this. I look forward to the record that develops and putting an end to this cyber fraud.

For their efforts to protect consumers and their privacy, thank you to Pam Arluk, Brian Cruikshank, Justin Faulb, Lisa Hone, Dan Kahn, Melissa Kinkel, Kris Monteith, and Christi Shewman of the Wireline Competition Bureau; Eduard Bartholme, Zac Champ, Aaron Garza, Eliot Greenwald, Kurt Schroeder, Mark Stone, Patrick Webre, and Kimberly Wild of the Consumer and Governmental Affairs Bureau; Ken Carlberg, Lisa Fowlkes, Jeffery Goldthorp, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Zenji Nakazawa, Erika Olsen, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Michael Epshteyn, James Graves, Phillip Rosario, Kimbarly Taylor, Kristi Thompson,

and Shana Yates of the Enforcement Bureau; Mark Azic, Patrick Brogan, Eugene Kiselev, Eric Ralph, and Emily Talaga of the Office of Economics and Analytics; and Doug Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel.